What is claimed is:

1. A method of alerting at least one device in a networked computer system comprising a plurality of devices to an anomaly, at least one of the plurality of devices having a firewall, comprising:

detecting an anomaly in the networked computer system;

determining which of the plurality of devices are anticipated to be affected by the anomaly; and

alerting the devices that are anticipated to be affected by the anomaly.

2. The method of claim 1, further comprising:

determining which of the plurality of devices have been affected by the anomaly; and

alerting the devices that have been affected by the anomaly.

3. The method of claim 1, further comprising adjusting the firewall of each of the devices that is anticipated to be affected by the anomaly responsive to the detection of the anomaly.

4. The method of claim 1, wherein the anomaly comprises one of an intrusion and an intrusion attempt.

5. The method of claim 1, wherein detecting the anomaly comprises analyzing a plurality of data packets with respect to predetermined patterns.

6. The method of claim 5, wherein analyzing the data packets comprises analyzing data packets that have been received at at least two of the plurality of devices.

7. The method of claim 1, wherein detecting the anomaly comprises recognition of an intrusion and further comprising generating an automated response to the intrusion.

8. A method of alerting a device in a networked computer system comprising a plurality of devices to an anomaly, comprising:

detecting an anomaly at a first device in the computer system;

determining a device anticipated to be affected by the anomaly; and

alerting the device that is anticipated to be affected by the anomaly.

9. The method of claim 8, wherein the plurality of devices are polled in a predetermined sequential order, the first device being polled prior to detecting the anomaly, and the device anticipated to be affected by the anomaly is a device that has not been polled.

10. The method of claim 8, further comprising transmitting an anomaly warning from the first device to a central analysis engine, responsive to detecting the anomaly at the first device, the anomaly warning comprising a unique device identifier.

11. The method of claim 8, wherein the anomaly comprises one of an intrusion and an intrusion attempt.

12. The method of claim 8, wherein detecting the anomaly comprises analyzing a plurality of data packets with respect to predetermined patterns.

13. The method of claim 12, wherein analyzing the data packets comprises analyzing data packets that have been received at at least two of the plurality of devices including the first device.

14. The method of claim 8, wherein alerting the device comprises alerting a firewall associated with the device that the anomaly has been detected.

15. The method of claim 8, wherein alerting the device comprises generating and transmitting an electronic notification to one of the device and an administrator of the device.

16. The method of claim 8, further comprising controlling the device that is anticipated to be affected by the anomaly.

17. An intrusion detection and alerting system for a computer network comprising:

a plurality of devices coupled to the computer network, each device adapted to at least one of: sense data and provide the data to a data collection and processing center, and be adjustable; and

the data collection and processing center comprising a computer with a firewall coupled to the computer network, the data collection and processing center monitoring data communicated to at least a portion of the plurality of devices coupled to the network, detecting an anomaly in the network, determining which of the devices are anticipated to be affected by the anomaly, and alerting the devices.

18. The system of claim 17, wherein the data collection and processing center further determines which of the devices have been affected by the anomaly and alerts the devices.

19. The system of claim 17, wherein at least one of the plurality of devices comprises a firewall, and the data collection and processing center further adjusts the firewall of each of the devices that is anticipated to be affected by the anomaly responsive to the detection of the anomaly.

20. The system of claim 17, wherein the anomaly comprises one of an intrusion, an intrusion attempt, and reconnaissance activity.

21. The system of claim 17, wherein the data collection and processing center detects the anomaly by analyzing a plurality of data packets with respect to predetermined patterns.

22. The system of claim 21, wherein the data collection and processing center analyzes data packets that have been received by at least two of the plurality of devices.